REMARKS

Claims:

Declaration:

The Examiner had indicated that the Third Declaration under 37 CFR 1.132 was "insufficient to overcome the rejection of claims 1-50 based on 35 U.S.C. 103(a)" because "it refers only to the system described in the above referenced application and not to the individual claims of the application. Thus, there is no showing that the objective evidence of nonobviousness is commensurate in scope with the claims."

Accordingly, the Declarant has prepared a Fourth Declaration under 37 CFR 1.132 that is specifically directed to the language employed in the claims.

35 U.S.C. 103(a):

Claims 1-50 stand rejected under 35 U.S.C. 103(a) based upon Anderl et al. (International Publication No. 87/07062) in view of Smith (U.S. Patent No. 4,956,769), and further in view of other patents for certain dependent claims. The additional cited patents are Davis (U.S. Patent No. 4,941,201), Wright et al. (U.S. Patent No. 6,084,969), Bapat et al. (U.S. Patent No. 6,038,563), and Hastings et al. (U.S. Patent No. 6,370,629).

The primary arguments made herein will concentrate on the fact that no combination of Anderl et al. and Smith describe or render obvious Applicant's invention, in that both are distinguished, and teach away, from Applicant's invention.

As a secondary point for certain dependent claims, it is difficult to understand how the combination of so many documents could be "obvious to one of skill in the art."

I) Claims 1, 15, 29 and 40:

Independent Claims 1, 15, 29 and 40 are separately rejected on similar grounds under 35 U.S.C. 103(a), the Examiner reciting Anderl et al. in view of Smith.

Anderl et al.:

The Examiner states, e.g. re Claim 1, that Anderl et al. teaches a portable data storage cartridge having a wireless interface and a computer processor. The Examiner also states that the computer processor receives the user authentication messages from the data storage drive via the wireless interface and transmits the user authorization or denial via the wireless interface.

However, the Examiner admits that "Anderl et al. does not teach the computer processor having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct with respect to the data storage media, the user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user; and combining the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity."

1a)

This same distinguishing feature of Applicant's invention is also pointed out by the accompanying Fourth Declaration under Rule 1.132, which points out that the card of Anderl et al. checks a password algorithmically against the appropriate

password at the same login level in the card header, but "any authentication (not directly described) appears to be of the 'card' or 'file' and not the 'user'".

"Thus, Anderl et al. access security is provided by an entirely different mechanism than the present '899 Application's claims 'combining said user authentication message with at least part of said user identifier from said user table in accordance with said predetermined algorithm, to authorize or deny said user activity.'

"Specifically, Anderl et al. have no 'user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media', and no ability to combine 'said user authentication message with at least part of said user identifier from said user table' of the claims of the present '899 Application."

1b)

Further, the accompanying Fourth Declaration under Rule 1.132 states "Anderl et al. appears to fail to provide a truly portable security access system. Rather, Anderl et al. discuss establishment of access at issuance by the issuer at a particular station. *** 'Each account in this example is handled by a separate file on the card and only persons or programs with the proper credentials for a particular file may access that file at an appropriate application station.' *** Thus, Anderl et al. access is established at issuance of the card, and management is limited to a particular station, making it non-portable, as opposed to the present '899 Application's claims 'combining said user authentication message with at least part of said user identifier from said user table in accordance with said predetermined algorithm, to authorize or deny said user activity', which allows fully portable access and management."

Smith:

The Examiner relies on Smith to provide these elements, the Examiner stating that "it would have been obvious" to have modified Anderl et al. in accordance with the teachings of Smith.

Further, in the response to arguments, the Examiner states that Smith "discloses a table having 'a first entry identifying the user'." Smith is said to "disclose the user signing onto a database and becoming authenticated. Column 5 further discloses parsing the system sign-on by the user and extracting a unique user identification symbol this symbol is then used to determine what operations the user is permitted to perform."

1c)

However, as pointed out by the accompanying Fourth Declaration under Rule 1.132, "Smith provides access tables or rules ***, but those tables do NOT RELATE to user authentication. Rather, any user authentication is a normal host system based logon process, using 'at least one system user, identified by a 'userid' or unique user identification symbol, that is accessing the system from at least one terminal location with a terminal address,' ***. Smith constructs a user access profile table and controls access 'by parsing the system sign-on by the system user and extracting therefrom the unique user identification symbol.' ***. The parsing is subsequent to the host system logon process and is not itself authentication." (Emphasis added).

"Smith is thus unlike the present '899 Application's claimed, e.g. Claim 1, 'user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user'.

"Thus, Smith does not add a portable security system to Anderl et al. related to the user table based authentication of the present '899 Application."

1d)

Further, the accompanying Fourth Declaration under Rule 1.132 states "Smith does not add portability of a security system to Anderl et al.

"Rather, *** Smith access is established at installation time, and is conducted within the host system, making it non-portable, as opposed to the claims of the present '899 Application which specify 'combining said user authentication message with at least part of said user identifier from said user table in accordance with said predetermined algorithm, to authorize or deny said user activity', which allows fully portable access and management."

2)

Applicant respectfully submits that Anderl et al. and Smith thus both are distinguished and teach away from Applicant's invention.

As further stated by the accompanying Fourth Declaration under Rule 1.132, "The combination of Anderl et al. and Smith teaches against the present '899 Application's 'portable security system comprising *** a computer processor mounted in said portable data storage cartridge ***; *** having a user table comprising at least a unique user identifier for each authorized user ***; said computer processor *** combining said user authentication message with at least part of said user identifier from said user table in accordance with said predetermined algorithm to authorize or deny said user activity ***.'

"Instead, the authorization of Smith is a normal sign-on within the host system, and is non-portable, and the Anderl et al. access security is provided by an entirely different mechanism, and is established at issuance of the card at a particular station, all as discussed above. Thus, both Smith and Anderl et al. teach against the portable authentication of the '899 Application."

3)

Applicant thus respectfully requests allowance of independent Claims 1, 15, 29 and 40 under 35 U.S.C. 103(a).

II) Claims 6, 20, 33 and 44:

The Examiner rejected Claims 6, 20, 33 and 44 on Anderl et al. in view of Smith stating that Anderl et al. teaches that the "user table permitted activities comprise a plurality of permitted activities, selected ones of which each of the users may be authorized to conduct, the permitted activities comprising *** 5) add entries to the user table, and 6) change/delete entries to the user table (see Smith ***)."

In the response to arguments, the Examiner states that, in Smith, a security administrator has the ability to define access privileges of users by the use of profiles and data access tables, and, since the administrator would be a user, "it is inherent" that "this user" can add, change and delete entries.

1)

Applicant respectfully submits that neither Anderl et al. nor Smith show or suggest the portable authentication of the '899 Application as discussed above with respect to Claims 1, 15, 29 and 40, and from which Claims 6, 20, 33 and 44 depend.

2)

Further, and as pointed out in the Third Amendment, Smith "does not provide management of access as part of an operational process, nor portability of that management. Rather, *** Smith access is established at installation time, and is conducted within the host system, making it non-portable, as opposed to the present '899 Application in which certain users are permitted management of access, and that access is portable. 'The permitted activities in the user table may comprise *** 5) add entries to the user table, and 6) change/delete entries to the user table.'"

Still further, and as pointed out in the Third Amendment, Anderl et al. "discuss establishment of access at issuance by the issuer at a particular station. *** 'The high security header 35 contains information such as *** the passwords for each login level ***. Direct access to the header section is available only to the two top security levels.' *** only persons or programs with the proper credentials for a particular file may access that file at an appropriate application station.'"

Therefore, Applicant respectfully submits that both Smith and Anderl et al. teach away from Applicant's invention, e.g. Claim 6, "The portable security system of Claim **1**, wherein said computer processor user table permitted activities comprise a plurality of permitted activities, selected ones of which each of said users may be authorized to conduct, said permitted activities comprising *** 5) add entries to said user table, and 6) change/delete entries to said user table."

Applicant thus respectfully requests allowance of Claims 6, 20, 33 and 44 under 35 U.S.C. 103(a).

III) Claims 8, 22, 35 and 46:

The Examiner rejected Claims 8, 22, 35 and 46 on Anderl et al. in view of Smith stating that Anderl et al. teaches that the "user table comprises a separate entry for each the user identifier, the entry comprising all the permitted activities the user is authorized to conduct (see Smith ***)."

In the response to arguments, the Examiner states that a discussion of Anderl et al. is insufficient since Anderl et al. cannot be taken alone since Anderl et al. is modified by Smith to disclose at least one unique user identifier for each authorized user.

1)

However, the rejected claims each depends from the respective independent claim as discussed above, and the authorization to gain access to the user table is submitted to be patentable over Smith and Anderl et al., as discussed above.

2)

Further, Anderl et al. is discussed in the Second Declaration under Rule 1.132 as "a fundamental distinguishing difference exists between the 'designated levels of interaction' of Anderl et al. and the present '899 Application's 'at least one unique user identifier for each authorized user'", and Smith is discussed in the Fourth Declaration under Rule 1.132 as providing "access tables or rules ***, but those tables do NOT RELATE to user authentication." (Emphasis added).

Applicant thus respectfully requests allowance of Claims 8, 22, 35 and 46 under 35 U.S.C. 103(a).

IV) Claims 9 and 23:

The Examiner rejected Claims 9 and 23 on Anderl et al. in view of Smith stating that Anderl et al. teaches that the "computer processor additionally comprises a nonvolatile memory storing the user table (see Anderl et al. ***)."

In the response to arguments, the Examiner's statement that a discussion of Anderl et al. is insufficient since Anderl et al. cannot be taken alone since Anderl et al. is modified by Smith to disclose at least one unique user identifier for each authorized user, also applies here.

1)

However, the rejected claims each depends from an independent claim which was discussed above, and the authorization to gain access to the user table is submitted to be patentable over Smith and Anderl et al., as discussed above.

2)

Further, Applicant respectfully submits that the "table" of Anderl et al. comprises "passwords for each security level are placed in the card header", and relate to designated levels of interaction between the card and the associated station without regard to the number of actual users at each level, as discussed above.

As pointed out above, in contrast, the "user table" of Claims 9 and 23 is defined as"comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct" in respectively Claims 1 and 15, from which Claims 9 and 23 depend.

Still further, Smith is discussed in the Fourth Declaration under Rule 1.132 as providing "access tables or rules ***, but those tables do NOT RELATE to user authentication."

Thus, Applicant respectfully submits that Claims 9 and 23 patentably define over Anderl et al. and Smith, and Applicant thus respectfully requests allowance of Claims 9 and 23 under 35 U.S.C. 103(a).

V) Claims 2 and 16:

Claims 2 and 16 have been rejected as being unpatentable over Anderl et al. and Smith in further view of Davis under 35 U.S.C. 103(a):

The Examiner states that Anderl et al. in view of Smith "does not teach wherein the wireless interface comprises an RF interface." Davis is said to teach "an RF interface". The Examiner further states "it would have been obvious *** to have modified Anderl et al. to include *** an RF interface. *** by the teachings of Davis ***".

In the response to arguments, the Examiner states that Davis "is only used to modify Anderl et al. to include the wireless interface is a RF interface".

1)

However, the rejected claims each depends from an independent claim which was discussed above, and the authorization to gain access to the user table is submitted to be patentable over Smith and Anderl et al., as discussed above.

2)

Applicant respectfully submits, that as pointed out by the first Declaration under Rule 1.132, "Davis has no ability to manage access" and therefore is submitted to be unable to make up for the distinguishing features of Applicant's invention over Anderl et al. and Smith as discussed above.

Hence, Applicant respectfully submits that Applicant's Claims 2 and 16 are therefore patentable over Anderl et al., Smith and Davis under 35 U.S.C. 103(a), and respectively requests allowance thereof.

VI) Claims 3-5, 17-19, 30-31 and 41-43:

The Examiner rejected Claims 3-5, 17-19, 30-31 and 41-43 under 35 U.S.C. 103(a) as being unpatentable over Anderl et al. and Smith in further view of Wright et al.

In the response to arguments, the Examiner states that Wright et al. "clearly teaches encryption/decryption during the authorization process."

A) Claims 3, 17, 30 and 41:

With respect to Claims 3, 17, 30 and 41, the Examiner states that Anderl et al. in view of Smith "does not teach wherein each the user identifier comprises a user symbol and a user decrypting key, wherein the user authentication message comprises an encrypted user authentication message which may be decrypted by the user decrypting key, and wherein the computer processor conducts the combination by decrypting the user authentication message by the user decrypting key." Wright et al. is said to teach "an encryption system for a two way pager" having the user identifier and encrypted user authentication message as above, and "wherein the computer processor conducts the combination by decrypting the user authentication message by the user decrypting key ***)." The Examiner further states "It would have been obvious *** to have modified Anderl et al. as modified, by the teachings of Wright et al. ***".

1)

However, Claims 3, 17, 30 and 41 depend from independent Claims 1, 15, 29 and 40 with respect to which Anderl et al. and Smith are submitted to teach away from Applicant's invention, as discussed fully above.

2)

Further, Applicant points out that Wright et al. is directed to communication of a pager, and does not have a user table, e.g. Claim 1, of "a computer processor mounted in said portable data storage cartridge". Rather, the pager has a single set of keys representing the pager and not separate users (column 7, lines 1-15), and communicates with a central "pager proxy server" (column 4, line 63 - column 5, line 25).

Hence, Applicant respectfully submits that Anderl et al., Smith and Wright et al. teach away from Applicant's use of encryption/decryption with the authorization process, e.g. Claim 3, "wherein each said user identifier comprises a user symbol and a user decrypting key, wherein said user authentication message comprises an encrypted user authentication message which may be decrypted by said user decrypting key, and wherein said computer processor conducts said combination by decrypting said user authentication message by said user decrypting key."

Therefore, Applicant respectfully and that therefore Applicant's Claims 3, 17, 30 and 41 are patentable over Anderl et al. in view of Smith and in further view of Wright et al. under 35 U.S.C. 103(a). Applicant therefore respectfully requests allowance of Claims 3, 17, 30 and 41.

B) Claims 4, 18, 31 and 42:

With respect to Claims 4, 18, 31 and 42, the Examiner states that Anderl et al. in view of Smith and in further view of Wright

et al. "teaches wherein the user decrypting key comprises a sender public key, and wherein the predetermined algorithm comprises a public key cryptographic algorithm ***."

1)

However, Claims 4, 18, 31 and 42 depend from Claims 3, 17, 30 and 41, wherein Anderl et al., Smith and Wright et al. are submitted to teach away from Applicant's use of encryption/decryption with the authorization process, which is submitted to not be overcome by the particular keys employed by Wright et al. in the communication process.

2)

Further, Claims 4, 18, 31 and 42 depend from independent Claims 1, 15, 29 and 40 with respect to which Anderl et al. and Smith are submitted to teach away from Applicant's invention, as discussed fully above.

Therefore, Applicant respectfully submits that Claims 4, 18, 31 and 42 are patentable over Anderl et al. in view of Smith and in further view of Wright et al. under 35 U.S.C. 103(a). Applicant therefore respectfully requests allowance of Claims 4, 18, 31 and 42.

C) Claims 5, 19, 32 and 43:

Claims 5 and 19, and Claims 32 and 43 are rejected separately and in similar fashion. The Examiner states that Anderl et al. in view of Smith and in further view of Wright et al. "teaches wherein the user authentication message is encrypted by a sender private key and a receiver public key ***, and wherein the public key cryptographic algorithm decrypts the user authentication message employing a receiver private key and the sender public key ***."

1)

However, Claims 5, 19, 32 and 43 depend from Claims 4, 18, 31 and 42, wherein Anderl et al., Smith and Wright et al. are submitted to teach away from Applicant's use of encryption/decryption with the authorization process, which is submitted to not be overcome by the particular keys employed by Wright et al. in the communication process.

2)

Further, Claims 5, 19, 32 and 43 depend from independent Claims 1, 15, 29 and 40 with respect to which Anderl et al. and Smith are submitted to teach away from Applicant's invention, as discussed fully above.

Therefore, Applicant respectfully submits that Claims 5, 19, 32 and 43 are patentable over Anderl et al. in view of Smith and in further view of Wright et al. under 35 U.S.C. 103(a). Applicant therefore respectfully requests allowance of Claims 5, 19, 32 and 43.

VII) Claims 7, 10-13, 21, 24-27, 34, 36-38, 45 and 47-49:

Claims 7, 10-13, 21, 24-27, 34, 36-38, 45 and 47-49 have been rejected as being unpatentable over Anderl et al. in view of Smith, and further in view of Bapat et al. under 35 U.S.C. 103(a).

The Examiner states in the response to arguments, that Applicant's arguments that Bapat et al. does not teach elements of Claims 1 and 6, were not considered because Bapat et al. was not mentioned in their rejection.

Applicant acknowledges that the discussion of Claim 6 was a non sequitur since the claims depend directly from the independent claims and not Claim 6.

1)

However, Bapat et al. Provides a "database access engine *** using the permissions table such that each user is allowed access only to management information in the set of database tables that the user would be allowed by the access control database to access." (column 3, lines 42-46), and does not provide a user identifier for authentication, and therefore is submitted to be unable to make up for the distinguishing features of Applicant's invention over Anderl et al. and Smith as discussed above.

Hence, Claims 7, 10-13, 21, 24-27, 34, 36-38, 45 and 47-49 are submitted to be patentable over Anderl et al. in view of Smith, and further in view of Bapat et al. under 35 U.S.C. 103(a).

A) Claims 7, 21, 34 and 45:

The Examiner states that, as to Claims 7, 21 and 45, Anderl et al. as modified by Smith does not teach a "user table comprises a separate entry for each the user identifier and the permitted activity the user is authorized to conduct", which is said to be taught by Bapat et al., and it "would have been obvious *** to have modified Anderl et al. as modified, by the teachings of Bapat et al. ***." Claim 34 is similarly rejected.

In the response to arguments, the Examiner states that Bapat et al. teaches having groups of users and it "is inherent that one of the groups of users would have to be able to read/write/change/modify/delete these lists".

1)

However, Bapat et al. isolates the permission tables from the creation or modification of the rules and definitions of the permission tables, none of which involves authentication (see FIGS. 4, 5 and 14). The rules and definitions are created or modified by the "Access Control Configuration procedure 210. The Access Control Configuration procedure 210 presents a graphical user interface 212 to users authorized to modify the access control tree 170." There is no indication of whom the Access Control Configuration procedure authorized users are nor where or how they are defined.

The Access Control Configuration procedure "users" are not authenticated nor are they defined or limited by the permission tables, which involve access requests. Thus, there is NO entry of permitted activities in the permission tables.

Hence, Applicant respectfully submits that Bapat et al. teaches away from, e.g. Claim 7, a "portable security system *** wherein said computer processor user table comprises a separate entry for each said user identifier and said permitted activity said user is authorized to conduct."

Further, Anderl et al. as modified by Smith have been discussed fully above.

2)

Further, Claims 7, 21, 34 and 45 depend from independent Claims 1, 15, 29 and 40 with respect to which Anderl et al. and Smith are submitted to teach away from Applicant's invention, as discussed fully above, and to which the modification by Bapat et al. additionally teaches away.

Applicant therefore respectfully submits that Claims 7, 21, 34 and 45 are patentable over Anderl et al. as modified by Smith

and as modified by Bapat et al. under 35 U.S.C. 103(a), and Applicant respectfully requests allowance thereof.

B) Claims 10, 24, 36 and 47:

With respect to Claims 10, 24, 36 and 47, the Examiner states that Anderl et al. as modified by Smith does not teach "a class table", but that Bapat et al. does teach a "class table comprising at least a unique class identifier for each authorized class of users ***, when combined with a user authentication message from a user of the authorized class of users ***, authorizes the user ***", and that it "would have been obvious *** to have modified Anderl et al. by the teachings of Bapat et al."

Further, the point of the Examiner in the response to arguments also applies to Claims 10, 24, 36 and 47, the Examiner stating that Bapat et al. teaches having groups of users and it "is inherent that one of the groups of users would have to be able to read/write/change/modify/delete these lists".

1)

Claims 10, 24, 36 and 47 depend from independent Claims 1, 15, 29 and 40 with respect to which Anderl et al. and Smith are submitted to teach away from Applicant's invention, as discussed fully above, and to which the modification by Bapat et al. additionally teaches away.

2)

Again, as discussed above, in Bapat et al., the rules and definitions of the permission tables are created or modified by the "Access Control Configuration procedure 210. The Access Control Configuration procedure 210 presents a graphical user interface 212 to users authorized to modify the access control

tree 170." There is no indication of whom the Access Control Configuration procedure authorized users are nor where or how they are defined.

The Access Control Configuration procedure "users" are not authenticated nor are they defined or limited by the permission tables, which involve access requests.

Hence, Applicant respectfully submits that Bapat et al. teaches away from, e.g. Claim 10, a "portable security system *** wherein said computer processor additionally comprises a class table comprising at least a unique class identifier for each authorized class of users and at least one permitted activity said class of users is authorized to conduct with respect to said data storage media, said class identifier, when combined with a user authentication message from a user of said authorized class of users in accordance with said predetermined algorithm, authorizes said user; and wherein said computer processor additionally, upon receiving said user authentication messages from said data storage drive via said wireless interface, combining said user authentication message with said class identifier from said class table in accordance with said predetermined algorithm to authorize or deny said class activity to said user, and transmitting said class authorization or denial to said data storage drive via said wireless interface." (Emphasis added).

Further, Anderl et al. as modified by Smith have been discussed fully above. Hence, Anderl et al. as modified by Smith and as modified by Bapat et al. are submitted to teach away from "combining said user authentication message with said class identifier" of Claims 10, 24, 36 and 47.

Applicant therefore respectfully submits that Claims 10, 24, 36 and 47 are patentable over Anderl et al. as modified by Smith and as modified by Bapat et al. under 35 U.S.C. 103(a), and respectfully requests allowance thereof.

C) Claims 11, 25, 37 and 48:

With respect to Claims 11, 25, 37 and 48, the Examiner states that Anderl et al. as modified by Smith and as modified by Bapat et al. teaches that the "user table additionally comprises any class membership of each the user".

1)

Claims 11, 25, 37 and 48 depend from Claims 10, 24, 36 and 47 which in turn depend from independent Claims 1, 15, 29 and 40, with respect to which Anderl et al. and Smith are submitted to teach away from Applicant's invention, as discussed fully above, and to which the modification by Bapat et al. additionally teaches away.

2)

As discussed above with respect to Claims 10, 24, 36 and 47, Anderl et al. as modified by Smith and as modified by Bapat et al. teach away from the Anderl et al. as modified by Smith and as modified by Bapat et al. are submitted to teach away from "combining said user authentication message with said class identifier" of Claims 10, 24, 36 and 47.

Claims 11, 25, 37 and 48 depend from Claims 10, 24, 36 and 47, and hence, Applicant respectfully submits that Bapat et al. teaches away from, e.g. Claim 11 "wherein said computer processor user table additionally comprises any class membership of each said user, wherein said user may be authorized with respect to said class table either by said class authorization or by said user authorization."

Applicant therefore respectfully submits that Claims 11, 25, 37 and 48 are patentable over Anderl et al. as modified by Smith

and as modified by Bapat et al. under 35 U.S.C. 103(a), and respectfully requests allowance thereof.

D) Claims 12, 26, 38 and 49:

With respect to Claims 12, 26 and 49, the Examiner states that Anderl et al. as modified by Smith and as modified by Bapat et al. teaches that the "user table and the class table permitted activities" include "3) read all entries of the class table, 4) add entries to the class table, and 5) change/delete entries to the class table". Claim 38 is similarly rejected.

1)

Claims 12, 26, 38 and 49 depend from Claims 10, 24, 36 and 47 which in turn depend from independent Claims 1, 15, 29 and 40, with respect to which Applicant submits Anderl et al. and Smith teach away from Applicant's invention, as discussed fully above, and to which the modification by Bapat et al. additionally teaches away.

2)

As discussed above with respect to Claims 10, 24, 36 and 47, Anderl et al. as modified by Smith and as modified by Bapat et al. teach away from the Anderl et al. as modified by Smith and as modified by Bapat et al. are submitted to teach away from "combining said user authentication message with said class identifier" of Claims 10, 24, 36 and 47.

Claims 12, 26, 38 and 49 depend from Claims 10, 24, 36 and 47, and hence, Applicant respectfully submits that Bapat et al. teaches away from Claims 12, 26, 38 and 49.

3)

Additionally, Applicant respectfully submits that, in Bapat et al., as discussed above, the permissions table is used to grant access to a database, and further submits that no "user" has access to the "permissions table", to, e.g., Claim 12, "3) read all entries of said class table, 4) add entries to said class table, and 5) change/delete entries to said class table."

Applicant therefore respectfully submits that Claims 12, 26, 38 and 49 are patentable over Anderl et al. as modified by Smith and as modified by Bapat et al. under 35 U.S.C. 103(a), and respectfully requests allowance thereof.

E) Claims 13 and 27:

With respect to Claims 13 and 27, the Examiner states that Anderl et al. as modified by Smith and as modified by Bapat et al. teaches a "nonvolatile memory storing the user table".

1)

Claims 13 and 27 depend from Claims 10 and 24, which in turn depend from independent Claims 1 and 15, with respect to which Anderl et al. and Smith are submitted to teach away from Applicant's invention, as discussed fully above, and to which the modification by Bapat et al. additionally teaches away.

2)

As discussed above with respect to Claims 10 and 24, Anderl et al. as modified by Smith and as modified by Bapat et al. teach away from the Anderl et al. as modified by Smith and as modified by Bapat et al. are submitted to teach away from "combining said user authentication message with said class identifier" of Claims 10 and 24.

Claims 13 and 27 depend from Claims 10 and 24, and hence, Applicant respectfully submits that Bapat et al. teaches away from, e.g. Claim 13 "wherein said computer processor additionally comprises a nonvolatile memory storing said user table and said class table."

Applicant therefore respectfully submits that Claims 13 and 27 are patentable over Anderl et al. as modified by Smith and as modified by Bapat et al. under 35 U.S.C. 103(a).

VIII) Claims 14, 28, 39 and 50:

The Examiner rejected Claims 14, 28, 39 and 50 under 35 U.S.C. 103(a) as being unpatentable over Anderl et al. and Smith in further view of Hastings et al. (U.S. Patent No. 6,370,629).

The Examiner states that Anderl et al. as modified by Smith "does not teach wherein the data stored in the data storage media is encrypted, and wherein the user authorization for the read access additionally comprises a decryption key for the encryption stored data."

The Examiner states that Hastings et al. teaches "wherein the data stored in the data storage media is encrypted ***, and wherein the user authorization for the read access additionally comprises a decryption key for the encrypted stored data ***."

Further, the Examiner states in the response to arguments, that Applicant's arguments that Hastings et al. does not teach elements of Claim 1 were not considered because Hastings et al. was not mentioned in their rejection.

1)

However, Applicant points out that Hastings et al. is directed to restricting use of information to designated geographic regions, and does not have a user table, e.g. Claim 1,

of "a computer processor mounted in said portable data storage cartridge". Rather, there are encrypted files with associated file decryption keys (column 4, lines 41-57), and that Hastings et al. does not provide a user identifier for authentication, and therefore is submitted to be unable to make up for the distinguishing features of Applicant's invention over Anderl et al. and Smith as discussed above.

Claims 14, 28, 39 and 50 depend from independent Claims 1, 15, 29 and 40 with respect to which Anderl et al. and Smith are submitted to teach away from Applicant's invention, as discussed fully above, and to which the modification by Hastings et al. additionally teaches away.

2)

Further, as discussed above, Hastings et al. is directed to restricting use of information to designated geographic regions, and does not have a user table related to an authorization process. Rather, there are encrypted files with associated file decryption keys (column 4, lines 41-57).

Hence, Applicant respectfully submits that Anderl et al., Smith and Hastings et al. teach away from Applicant's use of encryption/decryption with the authorization process, and that therefore Applicant's Claims 14, 28, 39 and 50 are patentable over Anderl et al. in view of Smith and in further view of Hastings et al. under 35 U.S.C. 103(a). Applicant therefore respectfully requests allowance of Claims 14, 28, 39 and 50.

SUMMARY:

Applicant respectfully submits that the present invention distinguishes over the cited patents and respectfully requests that the Examiner allow Applicant's Claims 1-50 under 35 U.S.C. 103.

Respectfully submitted,
P. J. Seger

By: _____
John H. Holcombe, (#20,620)
Attorney for Applicants

From: IBM Corporation
Intellectual Property Law
8987 E. Tanque Verde Rd. #309-374
Tucson, AZ 85749
Telephone: (520) 760-6629

JHH/cw

Attachment: Declaration